

DIALOG(R)File 351:Derwent WPI
(c) 2008 The Thomson Corporation. All rts. reserv.

0013197362

WPI ACC NO: 2003-281571/

XRPX Acc No: N2003-223678

Distributed denial of service attack protection system has attack shielding devices which are instructed by communication controller, when distributed denial of service attack is detected in network

Patent Assignee: NEC CORP (NIDE)

Inventor: HARAGUCHI M

1 patents, 1 countries

Patent Family

Patent Number	Kind	Date	Application Number	Kind	Date	Update
JP 2002158660	A	20020531	JP 2000355485	A	20001122	200328 B

Priority Applications (no., kind, date): JP 2000355485 A 20001122

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
JP 2002158660	A	JA	6	1	

Alerting Abstract JP A

NOVELTY - The attack detector (2) monitors and detects the distributed denial of service (DDoS) attack in the network (5), based on which a controller (3) instructs communication control to attack shielding devices (100-200). The base servers (300-400) control communication process, by receiving the communication control instruction and a certificate issuing unit (4) transmits the instruction to the attack shielding devices.

USE - Distributed denial of service (DDoS) attack protection system.

ADVANTAGE - Enhances the quality of service offered by performing large quantity access to a specific host server and protects against unauthorized access.

DESCRIPTION OF DRAWINGS - The figure shows a block diagram of the distributed denial of service (DDoS) attack protection system. (Drawing includes non-English language text).

2 attack detector

3 communication controller

4 certificate issuing unit

5 network

100-200 attack shielding devices

300-400 base servers

Basic Derwent Week: *200328*

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-158660

(P2002-158660A)

(43) 公開日 平成14年5月31日 (2002.5.31)

(51) IntCl. ⁷	識別記号	F I	テ-マコ-ト* (参考)
H 0 4 L 12/22		G 0 6 F 13/00	3 5 1 Z 5 B 0 8 9
G 0 6 F 13/00	3 5 1	H 0 4 L 11/26	5 K 0 3 0
H 0 4 L 29/14		13/00	3 1 1 5 K 0 3 5

審査請求 有 請求項の数 6 O L (全 6 頁)

(21) 出願番号 特願2000-355485 (P2000-355485)

(22) 出願日 平成12年11月22日 (2000.11.22)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 原口 稔

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100086645

弁理士 岩佐 義幸

Fターム(参考) 5B089 GA04 GB02 JA35 JB16 JB22

KA17 KB13 MC02 MC08

5K030 GA15 HB11 HC01 HC13 LB02

LB03 LD19 MB09 MC08

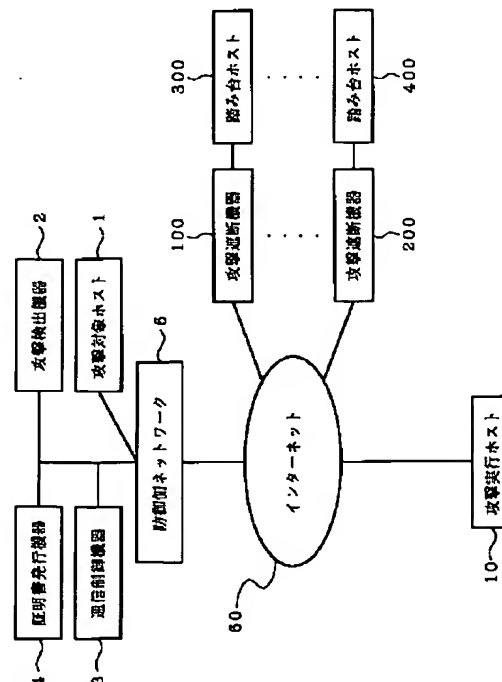
5K035 CC03 DD01 EE08 MM04

(54) 【発明の名称】 不正アクセス防御システム

(57) 【要約】

【課題】 特定のホストサーバに大量のアクセスを行って提供するサービスの品質を損なうDDoS攻撃に対応する現実的な防御手段を提供する。

【解決手段】 攻撃実行ホスト10の指示により踏み台ホスト300～400が攻撃対象ホスト1に対して大量のアクセスであるDDoS攻撃を実施すると、攻撃検出機器2は、防御側ネットワーク5の状況を監視してDDoS攻撃を検出し、通信制御機器3は、攻撃検出機器2がDDoS攻撃を検出した場合に、防御側ネットワーク5の管理者の指示により攻撃遮断機器100～200に通信制御の指示を出す。踏み台ホスト300～400は、通信制御の指示を受け取って通信を制御する。また、証明書発行機器4は、通信制御の指示の内容を保証する情報を攻撃遮断機器100～200に送信する。



1

【特許請求の範囲】

【請求項1】 防御側ネットワークの状況を監視して攻撃対象ホストに対する不正アクセスを検出する攻撃検出機器と、

前記攻撃検出器機が不正アクセスを検出した場合に、前記防御側ネットワークの管理者による通信制御指示を出す通信制御機器と、

物理的に離れた前記不正アクセスを実施するホストに所属し、前記通信制御指示を受け取って通信を制御する攻撃遮断機器と、を備えることを特徴とする不正アクセス防御システム。

【請求項2】 前記不正アクセスは、急激に増加するアクセスであることを特徴とする請求項1に記載の不正アクセス防御システム。

【請求項3】 前記攻撃遮断機器の通信を制御する責任が前記防御側ネットワークの管理者にあることを保証する情報を前記攻撃遮断機器に送信する証明書発行機器をさらに備えることを特徴とする請求項1または2に記載の不正アクセス防御システム。

【請求項4】 防御側ネットワークの状況を監視して攻撃対象ホストに対する不正アクセスを検出した場合に、防御側ネットワークの管理者の指示により、物理的に離れた前記不正アクセスを実施するホストに所属する攻撃遮断機器の通信を制御することを特徴とする不正アクセス防御方法。

【請求項5】 前記不正アクセスは、急激に増加するアクセスであることを特徴とする請求項4に記載の不正アクセス防御方法。

【請求項6】 前記攻撃遮断機器の通信を制御する責任が前記防御側ネットワークの管理者にあることを保証する情報を前記攻撃遮断機器に送信することを特徴とする請求項4または5に記載の不正アクセス防御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、特定のホストサーバへの不正なアクセスに対して防御を行う不正アクセス防御システムに関する。

【0002】

【従来の技術】 インターネットにおけるサービス妨害に、ターゲットとなるホストに多量のアクセスを行い負荷を増加させることによってターゲットとなるホストの提供するサービスの品質を損なう分散サービス拒否攻撃(DDoS攻撃: Distributed Denial of Service攻撃)による妨害がある。

【0003】 DDoS攻撃の特徴として、攻撃を行う側から直接攻撃対象のネットワークまたはホストに対して攻撃を行うのではなく、攻撃を行うためのエージェントプログラムをインターネット上の多数のサーバに設定し、それに対して攻撃指示を与えることでターゲットのネットワークに対して攻撃を行うという間接的な方法で

2

あることと、個々のアクセスは正当なアクセスであっても、アクセス量がターゲットとなったネットワークまたはホストの限界を越えた非常に多量のアクセスであることが問題となるため、攻撃が始まって以降の対応が難しいことがあげられる。

【0004】 DDoS攻撃の方式は、実行者のネットワーク環境の性能限界を越えたアクセスを実現するために実際に攻撃を行うホストを分散し、多数利用するために生み出された手法であるとも言える。

【0005】 従来、この種の「インターネットにおける分散サービス拒否攻撃に対するルータネットワークによる能動的な防御方法に関する発明」に相当する技術はなく、DDoS攻撃の踏み台に利用されないようにネットワークセキュリティを高めるか、特定パケットを一定量以上通過させないよう設定するかなど、何れも踏み台にされる側でセキュリティを高める方法のみが「2000年12月、情報処理振興事業協会発行、平成11年度電子計算機利用技術の高度化調査—インターネット先進利用技術に関する調査研究」および「2000年3月、日経オープンシステム、2000年3月号、オープンレポート、100頁」に発表されている。

【0006】 一旦、DDoS攻撃が開始されてからは、攻撃が終了するまで待つか、踏み台に利用されている多数ネットワークの管理者に対して個別にアクセスの遮断を依頼するかの方法しかない。

【0007】

【発明が解決しようとする課題】 しかしながら、上述した従来技術には、以下の問題点がある。

【0008】 第1に、現時点では攻撃を受ける側からの防御手段がないことである。DDoS攻撃への対応方法には、踏み台にされないようセキュリティを高める方法しか存在しないが、全てのネットワークがセキュリティを高め、かつそれを最新の状態に維持しない限り、踏み台にされうるネットワークはインターネット上に多数存在する。攻撃者は、手当たり次第に最新のセキュリティ対策を施されていないネットワークを探し、対策を施されたネットワークは単に無視すれば良い。

【0009】 第2に、攻撃が開始されてからの対応が事実上不可能ということである。攻撃が開始されたのを管理者が検知して以降は、攻撃を受けたネットワーク管理者から踏み台とされたホスト側に対して個別に対応を依頼する以外に対応方法がないが、数千台以上にのぼるホストの全管理者に対して依頼を行うのは事実上不可能である。

【0010】 本発明は、DDoS攻撃を受ける側からの責任において、DDoS攻撃が開始されて以降に本攻撃の影響を低減する方法を効率良く提供することを目的とする。

【0011】

【課題を解決するための手段】 本発明は、防御側ネット

3

ワークの状況を監視して攻撃対象ホストに対する不正アクセスを検出する攻撃検出機器と、前記攻撃検出機器が不正アクセスを検出した場合に、前記防御側ネットワークの管理者による通信制御指示を出す通信制御機器と、物理的に離れた前記不正アクセスを実施するホストに所属し、前記通信制御指示を受け取って通信を制御する攻撃遮断機器と、を備えることを特徴とする。

【0012】また、前記攻撃遮断機器の通信を制御する責任が前記防御側ネットワークの管理者にあることを保証する情報を前記攻撃遮断機器に送信する証明書発行機器をさらに備えることを特徴とする。

【0013】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0014】本発明は、インターネットにおけるDDoS攻撃に対して、ネットワーク上で通信経路の制御を、DDoS攻撃の被害者側からの責任および操作によって、新たなDDoS攻撃の発生に影響されることなく行う構成を提供するものである。

【0015】図1は、本発明の不正アクセス防御システムの実施の形態を示す構成図である。図1に示す不正アクセス防御システムは、攻撃対象ホスト1、攻撃検出機器2、通信制御機器3、証明書発行機器4、防御側ネットワーク5、攻撃実行ホスト10、インターネット50、攻撃遮断機器100～200、踏み台ホスト300～踏み台ホスト400とにより構成される。

【0016】攻撃対象ホスト1は、ワークステーション・サーバなどの情報処理装置である。攻撃対象ホスト1は、WWWサービスなどインターネット上にサービスを提供する機器として機能している。

【0017】攻撃検出機器2は、ネットワーク負荷監視装置である。防御側ネットワーク5の管理者は、本装置によりネットワークの利用状況を監視し、ネットワーク負荷が急激に増加した場合に、DDoS攻撃が発生したケースを想定し、ネットワーク負荷が増加した要因を調査し、その負荷がDDoS攻撃によるものかどうかを判断する。

【0018】DDoS攻撃の発生によるものであると判断された場合、攻撃検出機器2は、通信制御機器3に対してDDoS攻撃への対応指示を行う。

【0019】通信制御機器3は、防御側ネットワーク5上に設置されたワークステーション・サーバなどの情報処理装置である。通信制御機器3上では、通信制御の指示を出すためのアプリケーションソフトウェアが動作しており、攻撃検出機器2からの指示に従い、さらに攻撃遮断機器100～攻撃遮断機器200に対して攻撃実行ホスト10からの通信遮断指示を行うと同時に、証明書発行機器4に対して指示の妥当性の保証を依頼する。

【0020】証明書発行機器4は、防御側ネットワーク5上に設置されたワークステーション・サーバなどの情

4

報処理装置である。証明書発行機器4上では、通信制御機器3からの通信遮断指示が確かに防御側ネットワーク5の管理者から発行されたものであり、また、指示内容の改ざんが行われていないことを保証するための情報を攻撃遮断機器100～攻撃遮断機器200に対して送信する。

【0021】攻撃遮断機器100～攻撃遮断機器200は、ルータなどの情報処理装置である。攻撃遮断機器100～攻撃遮断機器200上では、通信制御機器3からの指示と証明書発行機器4からの通信を受け取るためのアプリケーションソフトウェアおよび指示された内容に従って任意のホストからの通信を遮断するためのアプリケーションソフトウェアが動作している。

【0022】踏み台ホスト300～踏み台ホスト400は、ワークステーション・サーバ・パーソナルコンピュータなどの情報処理装置である。踏み台ホスト300～踏み台ホスト400は、DDoS攻撃の実行者には本来利用できない機器であるが、DDoS攻撃の実行者によってインストールされたDDoS攻撃用ソフトウェアによってDDoS攻撃の実行者から操作可能となっている。

【0023】攻撃実行ホスト10は、ワークステーション・サーバ・パーソナルコンピュータなどの情報処理装置であり、DDoS攻撃の実行者から常に利用しうる状態となっている。

【0024】次に、図1に示す実施の形態の動作について説明する。

【0025】図1において、DDoS攻撃の実行者は、次の2つのステップを経てDDoS攻撃を行う。最初のステップは事前の準備であり、攻撃実行ホスト10を用いてインターネット50を経由して踏み台ホスト300～踏み台ホスト400にDDoS攻撃用ソフトウェアをインストールする。

【0026】次のステップでは、DDoS攻撃の実行者は、攻撃実行ホスト10から踏み台ホスト300～踏み台ホスト400に対して攻撃実行指示を行う。踏み台ホスト300～踏み台ホスト400は、その指示に従って攻撃対象ホスト1に対して一斉に大量のアクセスを行い、DDoS攻撃を行う。

【0027】それに対して、本発明では攻撃検出機器2・通信制御機器3・証明書発行機器4の構成により攻撃遮断機器100～攻撃遮断機器200に対してDDoS攻撃への防御指示を行い、DDoS攻撃からの防御を行う。

【0028】次に、図1に示す各構成機器の動作について、図1および図2を参照して説明する。図2は、各構成機器の動作を説明するフローチャートである。

【0029】攻撃検出機器2は、DDoS攻撃の発生を管理者からのネットワーク状況監視によって検出する。検出の手段としては、ネットワーク使用率の変化の監

視、サーバのCPU・メモリ・HDD利用率の変化の監視など、既存の普及したネットワーク・サーバ管理技術を用いて実現する。

【0030】攻撃対象ホスト1に対し、踏み台ホスト300～踏み台ホスト400までのホストを踏み台に利用したDDoS攻撃が発生したケースを想定して説明する。

【0031】・DDoS攻撃の発生

DDoS攻撃の実行者によって、攻撃実行ホスト10を用いて予めDDoS攻撃ソフトウェアのインストールされた踏み台ホスト300～踏み台ホスト400に対し、一斉に攻撃対象ホスト1に対する攻撃指示が出される。

【0032】・攻撃検出機器2

攻撃検出機器2は、防御側ネットワーク5の状況を監視する(ステップ100)。防御側ネットワーク5の管理者が、ネットワーク負荷が急激に増加したことを発見した場合、その原因となった通信を調査し、その結果、踏み台ホスト300～踏み台ホスト400からのアクセスが急激に増加したためであることを検出する(ステップ101)。管理者は、通信制御機器3に対して踏み台ホスト300～踏み台ホスト400からの通信を遮断するよう、通信制御機器3に対して指示を行う(ステップ102)。

【0033】・通信制御機器3

通信制御機器3は、攻撃検出機器2の指示に従い、踏み台ホスト300～踏み台ホスト400に対する通信遮断を行うよう攻撃遮断機器100～攻撃遮断機器200に対して指示を行う(ステップ106)。また、証明書発行機器4に対して通信遮断指示の内容保証を依頼する(ステップ103)。

【0034】・証明書発行機器4

RSA公開鍵暗号化方式など既存の認証技術を用いて通信制御ブロックからの通信内容が正当なものであり、かつ改ざんされていないことを証明し、証明結果を攻撃遮断機器100～攻撃遮断機器200に対して送信する(ステップ104)。

【0035】・攻撃遮断機器100～200

踏み台ホスト300～踏み台ホスト400が所属する個々のネットワークのうち攻撃遮断機器を備えたネットワークにおいて、通信制御機器3からの指示内容の妥当性を確認した後(ステップ105)、指示に従い踏み台ホスト300～踏み台ホスト400からの通信を遮断する(ステップ107)。

【0036】例えば、踏み台ホスト300～踏み台ホスト400の所属する個々のネットワークのうち8割のネットワークにおいて、攻撃遮断機器100～攻撃遮断機器200が本発明に対応した攻撃遮断装置を実装していた場合、攻撃対象ホスト1への影響はそれまでの2割まで低減され、攻撃対象ホスト1は、DDoS攻撃発生以前に比べサービスが稼働可能な許容範囲内にまで復帰す

ることが可能となる。

【0037】一定期間の経過後(ステップ108)、踏み台ホスト300～踏み台ホスト400に対する通信遮断を解除する(ステップ109)。

【0038】本発明の特徴は、従来、DDoS攻撃に対する防御方法として踏み台ホスト300～踏み台ホスト400が攻撃用ソフトウェアをインストールされないことで対応しようとしていたことに対して、踏み台ホスト300～踏み台ホスト400に攻撃用ソフトウェアがインストールされた場合でも、攻撃遮断機器100～攻撃遮断機器200においてDDoS攻撃の影響を無視できる範囲に低減することにある。

【0039】本発明は、ネットワークを経由したサービス妨害に対して妨害行為を受ける側の判断と責任によって妨害行為を強制的に中断させるものである。従って、DDoS以外の応用としては不正アクセス全般に対して本システムを適用することが可能である。次に、応用例として本システムをポートスキャンに適用した場合について説明する。

【0040】・攻撃検出機器2

管理者からのネットワーク監視によってポートスキャンを検出することにより、他のブロックに対してポートスキャンへの対応指示を行う。

【0041】・通信制御機器3

攻撃検出機器2の指示に従って攻撃遮断機器100～攻撃遮断機器200に対し、不正アクセスの発生したホストからの通信を遮断するよう指示を行う。

【0042】・証明書発行機器4

通信制御機器3からの通信が正当なものであることを保証し、通信制御を実施することの責任が攻撃遮断機器100～攻撃遮断機器200の管理者でなく防御側ネットワーク5の管理者にあることを保証する。

【0043】・攻撃遮断機器100～攻撃遮断機器200

通信制御機器3からの指示に従って、不正アクセスの発生したホストからの通信経路を遮断する。

【0044】上記応用例ではポートスキャンについて示した。この最初のきっかけとなる不正アクセスの検出を他の不正アクセス検出方式で置き換えることで、検出可能な全ての不正アクセスに対して不正アクセスの被害を被る立場からの能動的な通信遮断が可能である。

【0045】ただし、不正アクセスとみなしたホストからの通信が本当に不正アクセスなのか、何らかの理由による正当なアクセスなのかについての判断は、不正アクセスを受けた側での判断と責任において行うものであることに留意し、必要なアクセスを遮断させることにより通信相手に対して損害を与えないよう注意する必要がある。

【0046】

【発明の効果】以上説明したように、本発明は、従来、

7

攻撃対象とされた場合に対応不可能と言われていたDDoS攻撃に対して対応する現実的な手段を提供する。基本的には、インターネットを構成するネットワーク全てが本システムに対応することが望ましいが、大規模な回線業者などインターネット上での通信の基幹部分にあたるネットワークにおいて本システムを適用することで、DDoS攻撃の最大の特徴である膨大な量の通信を許容できる量の通信に抑えることが可能である。

【0047】また、本発明においては、DDoS攻撃に対応する場合の主体が被害を受ける当事者にあるということである。従来のDDoS攻撃への対応方法は、インターネットを構成する全てのネットワークにおいて対応することを要求とし、その責任が最新のセキュリティ技術を用いていなかった別の企業にあったとしても、当事者からそれに対する責任を問うシステムは確立されていない。

【0048】本発明においては、最新のDDoS攻撃に対応し得るかどうかは不正アクセスの対象となる当事者がそれを検出し得るかどうか、という当事者の責任において行うことが可能である。

【0049】また、本発明においては、基本的に技術の更新が不要であることである。一般に、ネットワークまたはホスト単体において不正アクセスに対応したとしても、次々と新しい不正アクセスが発生し、常にネットワークまたはホスト単体を最新のセキュリティ技術を適用*

8

*する必要がある。本発明においては、当事者の責任において当該不正アクセスに対する遮断を指示することを可能としているため、継続的に本技術を利用し続けることが可能である。

【0050】インターネットを構成するネットワーク機器全てに最新のセキュリティ技術が導入されるかどうかは、それを運営する企業判断に任されている以上、一度導入すれば更新する必要のない本発明は、不正アクセスに対する現実的な対応方法を提供することが可能である。

【図面の簡単な説明】

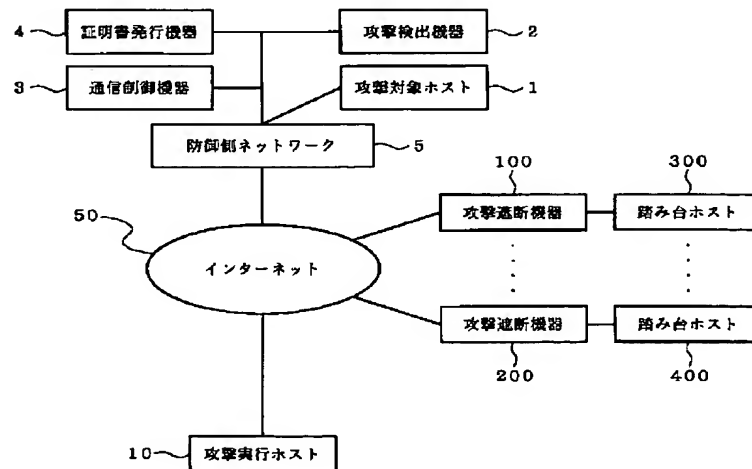
【図1】本発明の不正アクセス防御システムの実施の形態を示す構成図である。

【図2】図1に示す各構成機器の動作を説明するフローチャートである。

【符号の説明】

- 1 攻撃対象ホスト
- 2 攻撃検出機器
- 3 通信制御機器
- 4 証明書発行機器
- 5 防御側ネットワーク
- 10 攻撃実行ホスト
- 50 インターネット
- 100 攻撃遮断機器
- 200 攻撃遮断機器
- 300 踏み台ホスト
- 400 踏み台ホスト

【図1】



【図2】

